



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/800,505	03/08/2001	Seigo Kotani	1405.1036	2180

21171 7590 02/13/2006

STAAS & HALSEY LLP
SUITE 700
1201 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20005

EXAMINER

SIMITOSKI, MICHAEL J

ART UNIT PAPER NUMBER

2134

DATE MAILED: 02/13/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/800,505

Applicant(s)

KOTANI ET AL.

Examiner

Michael J. Simitoski

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 29 November 2005.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-29 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-29 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 08 March 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. The response of 11/29/2005 was received and considered.
2. Claims 1-29 are pending.

Response to Arguments

3. Applicant's arguments filed 11/29/2005 have been fully considered but they are not persuasive and as such, the art of record suggests that the current claims are not yet patentable.
4. In light of Applicant's amendments to the claims, the rejections under §112 ¶2, set forth in the previous Office Action, are withdrawn.
5. Applicant's response (p. 7) argues that neither Hasebe, Ginter, Chen nor Shear disclose or suggest "storing the encrypted predetermined information in an area outside said predetermined secure area." However, Hasebe discloses storing permissions information on a recording medium (portable card) (Fig. 2). Chen teaches that it is useful in reducing costs, to occasionally backup the data on an IC card to a storage medium (p. 1, ¶1-3) and therefore it is submitted that it would have been obvious to modify Hasebe to backup the permission information on the portable card. Hence, Hasebe, as modified above, teaches storing the encrypted predetermined information in an area outside said predetermined area (in a backup storage medium).
6. Applicant's response (p. 8, ¶2) argues that Chen's IC card has no encrypted predetermined information to store. However, the information stored on Chen's IC card does not change the teaching that it can be beneficial to backup data stored on a recording medium.
7. Applicant's response (p. 8) argues that Ginter does not teach the above limitation. However, Ginter is not cited for teaching "storing the encrypted predetermined information in an

area outside said predetermined secure area". Rather, Ginter is cited for teaching that is it well known, when backing up data or keys on a storage medium, to encrypt the data with a public key associated with the storage medium (col. 173, lines 44-56).

8. Applicant's response (pp. 8-9) argues that Shear does not teach the above limitation. However, Shear is not cited for teaching "storing the encrypted predetermined information in an area outside said predetermined secure area". Rather, Shear is cited for explicitly teaching that it is well known to store data in a hidden area of the disc. While little patentable weight is given to the phrase "secure area", as it is not a standard term and the claim does not define it further, Hasebe does not explicitly disclose that the area in which the permissions information is stored is a "secure area". Shear teaches that it is useful to store certain data in a hidden area, which is inaccessible to certain readers (p. 15, ¶218).

9. Applicant's response (p. 9) argues that one of ordinary skill would have been deterred from modifying Hasebe in the manner proposed because Hasebe "warns against illegal copying". However, Hasebe's invention solves this problem by encrypting the data, which does not affect the combination proposed. As such, the permissions information would benefit from being backed up, as a method to reduce storage costs.

10. Applicant's response (pp. 10-11) argues that neither Hasebe, Ginter, Chen, Shear nor Lang shows "storing the encrypted predetermined information in an area outside said predetermined secure area". This argument was addressed above.

11. Applicant's response (p. 11) argues that new claim 29 recites "storing information encrypted with medium-specific information or a key generated therefrom in an area outside a

Art Unit: 2134

secure area” and as such is allowable. However, Schneier discloses storing information/Alice’s message encrypted with medium/Bob-specific information/Bob’s public key in an area/Alice outside a secure area/Bob and deriving/using said encrypted information outside said secure area (p. 32).

Claim Rejections - 35 USC § 102

12. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

13. Claim 29 is rejected under 35 U.S.C. 102(b) as being anticipated by Applied Cryptography, Second Edition by **Schneier**. Schneier discloses storing information/Alice’s message encrypted with medium-specific information/Bob’s public key in an area/Alice outside a secure area/Bob and deriving/using said encrypted information outside said secure area (p. 32).

Claim Rejections - 35 USC § 103

14. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

15. Claims 1-7, 9, 11, 13, 18-19, 21, 23 & 25-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent 5,392,351 to Hasebe et al. (**Hasebe**) in view of U.S. Patent 5,892,900 to Ginter et al. (**Ginter**), UK Patent Application GB 2 284 689 A to **Chen** and U.S. Patent Application Publication 2001/0042043 to Shear et al. (**Shear**).

Regarding claims 1-3, 11, 19, 23 & 27-28, Hasebe discloses predetermined information/permission information stored in a predetermined secure area of a recording medium (Fig. 2, #13), but lacks explicitly a secure area, lacks encrypting the predetermined information using medium-specific information, lacks storing the encrypted information in an area outside the secure area and lacks explicitly deriving said encrypted predetermined information outside said predetermined secure area. However, Chen teaches that to reduce cost in operating an IC card, it is beneficial to backup the data on the IC card to a storage medium (p. 1, ¶1-3). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Hasebe to store the predetermined information/permission information outside the predetermined area and to derive the information outside said predetermined area. One of ordinary skill in the art would have been motivated to perform such a modification to backup the predetermined information to reduce costs, as taught by Hasebe (p. 1, ¶1-3). Further, Ginter teaches that when backing up data/keys on a storage medium/SPU, it is known to encrypt the data with a public key associated with the storage medium/SPU to secure the keys (col. 173, lines 44-56). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Hasebe to encrypt the backed up predetermined information/permission information with a medium-specific key or key derived therefrom. One of ordinary skill in the art would have been motivated to perform such a

Art Unit: 2134

modification to secure the backed up permission information, as taught by Ginter (col. 173, lines 44-56). Further, Shear teaches that keys can be contained in a hidden area on a disc, not normally accessible so that an attempt to copy the disc would not copy the keys (p. 15, ¶218). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Hasebe to include a secure area for storing the predetermined information, the secure area not subject to control by external instructions. One of ordinary skill in the art would have been motivated to perform such a modification to prevent copying of the predetermined information, as taught by Shear (p. 15, ¶218).

Regarding claims 4-5 & 7, Hasebe, as modified above, discloses storing encrypted electronic data in the second area (Fig. 2, #14) and license information based on use rights for using the electronic data in the first area (Fig. 2, #13).

Regarding claims 6 & 9, Hasebe, as modified above, lacks encrypting the predetermined information/permission information with explicitly information specific to an apparatus that drives said recording medium (or a key generated therefrom). However, Shear teaches using keys to protect 'metadata' that is used to determine access properties to 'property' on a storage medium (Fig. 3) by an access apparatus. The keys on the storage medium are encrypted with a key(s) specific to the apparatus so the keys in the encrypted key block are not exposed (Fig. 3 & p. 15 ¶219). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to encrypt the predetermined information with a key specific to the driving apparatus. One of ordinary skill in the art would have been motivated to perform such a modification to prevent keys/data from being exposed, as taught by Shear (Fig. 3 & p. 15 ¶219).

Art Unit: 2134

Regarding claims 13, 21, 25 & 26, Hasebe discloses a system, as described above (Fig. 13 & col. 10 lines 50-59), but lacks further encrypting the predetermined information/permission information with information specific to an apparatus that drives the second recording medium (or a key generated therefrom). Regarding claim 26, Hasebe discloses a second recording medium (Fig. 13). However, Shear teaches using keys to protect 'metadata' that is used to determine access properties to 'property' on a storage medium (Fig. 3). The keys on the storage medium are encrypted with a key(s) specific to the apparatus so the keys in the encrypted key block are not exposed (Fig. 3 & p. 15 ¶219). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to further encrypt the predetermined information with a key specific to the driving apparatus. One of ordinary skill in the art would have been motivated to perform such a modification to prevent keys/data from being exposed, as taught by Shear (Fig. 3 & p. 15 ¶219).

Regarding claim 18, Hasebe discloses an apparatus/vendor computer (Fig. 2) with a stored medium with medium-specific information/medium number (Fig. 2 #12) and comprising a user-use area allowing reading out of information/permission information (Fig. 2), the apparatus/computer managing information of a recording medium wherein license information/permission information based on use rights for any information stored in a user-use area is stored in an area (Fig. 2) and write and read out means/vendor computer and user computer transferring information to and from a user-user area predetermined information deriving means/vendor computer (Fig. 7A) stored in the area. Hasebe further discloses reading/user computer and writing means/vendor computer (Fig. 2) to read and write to the user-use area and encrypting permission information with medium-specific information/medium

Art Unit: 2134

number (Fig. 2 #12, 21, 23, 22 & 13). Hasebe lacks explicitly a secure area, lacks encrypting the predetermined information using medium-specific information, lacks storing the encrypted information in an area outside the secure area and lacks explicitly deriving said encrypted predetermined information outside said predetermined secure area. However, Chen teaches that to reduce cost in operating an IC card, it is beneficial to backup the data on the IC card to a storage medium (p. 1, ¶1-3). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Hasebe to store the predetermined information/permission information outside the predetermined area and to derive the information outside said predetermined area. One of ordinary skill in the art would have been motivated to perform such a modification to backup the predetermined information to reduce costs, as taught by Hasebe (p. 1, ¶1-3). Further, Ginter teaches that when backing up data/keys on a storage medium/SPU, it is known to encrypt the data with a public key associated with the storage medium/SPU to secure the keys (col. 173, lines 44-56). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Hasebe to encrypt the backed up predetermined information/permission information with a medium-specific key or key derived therefrom. One of ordinary skill in the art would have been motivated to perform such a modification to secure the backed up permission information, as taught by Ginter (col. 173, lines 44-56). Further, Shear teaches that keys can be contained in a hidden area on a disc, not normally accessible so that an attempt to copy the disc would not copy the keys (p. 15, ¶218). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Hasebe to include a secure area for storing the predetermined information, the secure area not subject to control by external instructions. One

Art Unit: 2134

of ordinary skill in the art would have been motivated to perform such a modification to prevent copying of the predetermined information, as taught by Shear (p. 15, ¶218).

16. Claims 8, 10, 12, 14-17, 20, 22 & 24, as best understood, are rejected under 35 U.S.C. 103(a) as being unpatentable over **Hasebe, Ginter, Chen and Shear**, as applied to claims 1 & 11 above, in further view of U.S. Patent 5,191,611 to **Lang**.

Regarding claim 8, 10, 12, 14, 20, 22 & 24, Hasebe, as modified above, lacks updating the predetermined information/permission information. However, Lang teaches that to authorize a user a specific number of information retrievals, a personal access device (PAD) can receive an update command reflecting the users' updated privileges (col. 12 lines 36-58). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to enable the updating of the predetermined information. One of ordinary skill in the art would have been motivated to perform such a modification to limit data retrievals by users, as taught by Lang (col. 12 lines 36-58). Further, it is inherent, based on the key(s) used for encryption, that decryption will use the same key(s).

Regarding claim 15, Hasebe, as modified above, lacks the medium-specific information/medium number being visually displayed on the recording medium. However, Lang teaches that by displaying information visually on a device for controlling access to data, a user can manually enter the data into another device (col. 6 lines 55-59). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to visually display the medium-specific information/medium number on the recording medium. One of ordinary skill in the art would have been motivated to perform such a modification to

allow for manual entry of the medium-number into another device, as taught by Lang (col. 6 lines 55-59).

Regarding claims 16 & 17, Hasebe, as modified above, lacks the apparatus-specific information being visually displayed on the apparatus. However, Lang teaches that by displaying information/code visually on a device/smart card for controlling access to data, a user can manually enter the data into another device (for key generation and challenge-response identification) (col. 6 lines 55-59 & col. 7 lines 44-65). Lang further discloses electronic transmission from the smartcard to another device such as a reader (col. 12 lines 53-58). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to visually display the information specific to an apparatus on the apparatus. One of ordinary skill in the art would have been motivated to perform such a modification to allow for user access to the apparatus-specific information for entry into another device to derive a key or entertain challenge-response identification, as taught by Lang (col. 6 lines 55-59 & col. 7 lines 44-65).

Conclusion

17. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period

Art Unit: 2134

will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

18. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (571) 272-3841. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m.. The examiner can also be reached on alternate Fridays from 6:45 a.m. - 3:15 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached at (571) 272-3838.

Any response to this action should be mailed to:

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Or faxed to:

(571) 273-8300
(for formal communications intended for entry)

Or:


(571) 273-3841 (Examiner's fax, for informal or draft communications, please label "PROPOSED" or "DRAFT")

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571) 272-2100.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).


MJS

February 6, 2006


GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100